Wicked node detection in wireless ad-hoc network by applying supervised learning

Chitra Sabapathy Ranganathan[1], Rajeshkumar Sampathrajan[2]
[1]Information Technology, Mphasis Corporation Chandler, Arizona, United States
[2]Cloud Architect, McKinsey and Company, Fort Worth, Texas, United States

Article Info

Article history:

Received Oct 4, 2023
Revised Mar 12, 2024
Accepted Mar 15, 2024

Keywords:

Internet of things
Linear correlation coefficient
Support vector machine
Wireless ad-hoc network
Wicked nodes detection

ABSTRACT

A wireless ad-hoc network (WANET) is a decentralized network supported by wireless connections without a pre-existing architecture. However, the mobility of nodes is a defining characteristic of WANETs, and the speed with which nodes may act poses several security risks. As a result of these wicked nodes, more data packets are lost, which might cause a significant delay. Thus, it is very important to identify wicked nodes in WANET. This work provides a support vector machine approach for detecting (SVMD) wicked nodes in the internet of things. The number of characteristics is reduced using the linear correlation coefficient (LCC) technique. With the LCC technique, we can precisely measure the strength of the connection between any two nodes while clearing the field of irrelevant information. Further, the support vector machine (SVM) algorithm may identify the wicked nodes by analyzing metrics such as the packet received ratio, packet delay ratio, and remaining energy ratio. The next step is to reach a verdict in which the wicked nodes are punished by being rendered inoperable. The simulation results show that the network latency is minimized, and the chance of missing detection is decreased using this method in WANET.

Corresponding Author:

Chitra Sabapathy Ranganathan
Information Technology, Mphasis Corporation
Chandler, Arizona, United States
Email: chitrasabapathyranganathan@gmail.com

1. INTRODUCTION

A wireless ad-hoc network (WANET) is a leading technology for executing the internet of things (IoT) structure [1]. Several approaches utilize for transmission, and messaging are the key necessities of an IoT system. IoT is a promising dynamic cyber-physical network that facilitates smart devices to supervise and modify the world. WANET faces recognized problems because operations in harsh and unattended surroundings, like attackers, can attack the network by cooperating with the sensor nodes with sensitive information like identity and position [2]. The interaction of IoT with WANET is vulnerable to a diversity of attacks that could damage security. The identification is utilized in cryptographic operations like encryption and decryption. Though, this identification is altered through actually accessing the nodes. Thus, many investigators introduced different approaches to concentrate on this problem. Support vector machine (SVM) is a machine learning technique that complements the intrusion detection system function and minimizes false alarms [3]. SVM is a better classification technique in security applications like identification of wicked, intrusion recognition, and spam filtering [4]. But, SVM can integrate with real-world security and cope with attack patterns to mislead the learning method. The SVM kernel operations established classifiers to differentiate the malevolent nodes from kind ones by measuring the variance in their driving pattern matrices

[5]. This approach can reach a low error rate with a high detection rate. The SVM method categorizes normal and abnormal network nodes [6].

Problem statement: Wireless IoT devices applying low power and lossy networks lacking centralized security management are enormously susceptible to attacks, as a wicked node can falsify several identities and perform attacks. Many approaches have been examined to avoid attacks; however, vital restrictions remain. A physical identification-based trust path routing (PITrust) approach applies the received signal strength indicator and a centralized trust method to enhance attack detection and improve the packet delivery ratio [7]. However, this approach cannot enhance the wicked node detection in the network.

Work contribution: The wicked nodes detection system is intended to distinguish and perform against network violations by observing and recognizing abnormal nodes. Thus, it ensures the accessibility and reliability of the network services; it is critical to have this system executed and managed effectively. This article proposes an SVM algorithm to detect wicked nodes (DWN) by incorporating the SVM algorithm. In this approach, the linear correlation coefficient (LCC) method minimizes the number of features. The LCC method perfectly measures the connection between two nodes and removes unnecessary data. The SVM algorithm isolates the wicked nodes based on the packet received ratio, packet delay ratio, and remaining energy ratio. SVM algorithms make a decision that gives the punishment in terms of the jamming of the wicked nodes.

The structure of the remaining parts of the article is as follows: section 2 describes the SVM-based system to detect wicked nodes in IoT WANET. Next, simulation results are specified in section 3, and it compares packet received ratio, delay, remaining energy and miss detection possibility. Finally, the article's conclusion is in section 4.

The selective forwarding attack (SFA) is the most difficult attack to recognize between denial-of-service attacks. The wicked nodes initiate the SFA that losses some data packets. Here, an artificial immune system established the danger model to detect SFA attacks [8]. SVM is a supervised machine learning that provides great execution and classification role with great dimensional data. It has a small expected simplification error. The machine learning model uses an SVM algorithm to determine the attack in the network. Three SVM kernel operations utilized the classifiers to differentiate the malevolent nodes from reliable ones by measuring the variance [9]. A malicious-node identification approach applying a correlation procedure avoids fault data injection attacks. Initially, the time correlation procedure identified abnormal sensor nodes among neighbor nodes. Next, the wicked nodes are determined by applying the spatial correlation method. Finally, the event correlation procedure identified the wicked nodes efficiently [10]. The max-min method is utilized to compute a corresponding fused value of nodes. This assists in declining the manipulation of a fault node on wicked node recognition and enhances the recognition accuracy. However, this approach cannot use the machine learning concept; thus, it cannot efficiently detect wicked nodes. In addition, this approach does not include the IoT. Furthermore, it minimized the energy efficiency in the network [11]. A reinforcement learning algorithm is used to detect the selective forwarding attack. The double-threshold density peaks clustering method identified wicked nodes [12].

Authentication is mostly for secure transactions. It is the procedure of verifying if the transmitter is a reliable one; otherwise, not also to verify the trustiness of the message obtained, which is to see if the messages are updated through others outside the network or the group [13]. In the symmetric key method, the transmitter and the recipient should have the stealthy key confidently. In other words, do not deliver security to the technique; offer protection only to the key [14]. A primary identity-based cryptography approach has three issues. Initially, non-public key generation is presumed trusty and aware of all nodes' non-public keys. Next, the unique identity for each node reasons the incapability to apprise keys inside the case of cooperation. Finally, a secure channel is essential for reassigning non-public keys [15]. The extended identity-based encryption approach ensures authentication and confidentiality. The Kerberos authentication approaches and identity-based encryption confirm authentication and privacy [16]. The Diffie-Hellman convention utilizes elliptic curve cryptography, both elliptic open and sealed keys, to construct a mutual secret key over an indeterminate channel. Advanced encryption standard algorithm for encrypting and decrypting the information ensures security. This approach does not utilize the machine learning algorithm [17], [18]. More secure and efficient access control allows an internet user in certificate-less cryptography to transmit with a sensor node in identity-based cryptography surroundings with dissimilar system parameters. Furthermore, this approach attains specific temporary information security [19]. The secure and privacy-aware approach recognizes the attacker by offering the digital security certificate. This certificate offers the nodes and allows certified nodes to contribute to the route communicating the packets from the sender to the receiver. This efficient approach is recognized for utilizing more time [20].

A classification technique in that the decision for the class association is established on exact combinations of attributes states here and those mixtures are stimulated by reliability. Incorporate machine learning into the simulation-based consistency evaluation approach, and evaluate the system consistency experimentally [21]. The core reliability evaluation system is a supervised learning method named perception, a state-space classification-based approach for system state evaluation. It detects the intrusion by the node's signal strength. In source embarrassed IoT devices, energy maintenance also small handling load between the most serious problems. Mainly, classical approaches are utilized for detecting and avoiding attacks [22]. A received signal strength indications (RSSI) possesses the energy communication operation; communication energy will source it to construct diverse RSSI. Applying the RSSI ratio values can precisely distinguish the sybil attack [23]. A Bayesian thresholding algorithm is forecast the received signal strength and link reliability for describing wicked. The hill climbing with cuckoo search algorithms can reach the best solutions by applying fitness functions [24]. An end-to-end data delivery reliability framework catching the ratio of received packet, noise for background, and RSSI [25]. Cooperative routing for improving lifetime objectives to improve the lifetime and reduce the cost of route detection. This mechanism utilizes the fresher encounter algorithm to enhances the lifetime [26]. A link expiration time-aware routing mechanism offers lesser energy utilization and it reaches the packet reliability [27]. Energy aware routing mechanism to reduce energy expenditure and select preferred next hop by measuring the link quality by node energy, and quality of link to improve the data transmission, and reduce the energy expenditure [28].

2. PROPOSED METHOD

This approach contains a data collection phase, data preprocessing phase, quality of service (QoS) computation phase, and SVM-based categorization phase. Figure 1 demonstrates the SVM algorithm operation for detecting wicked nodes. In a WANET, information is gathered from the data source. The data collection phase gathers important information from the source of data. The preprocessing data phase is accountably minimizing the features.

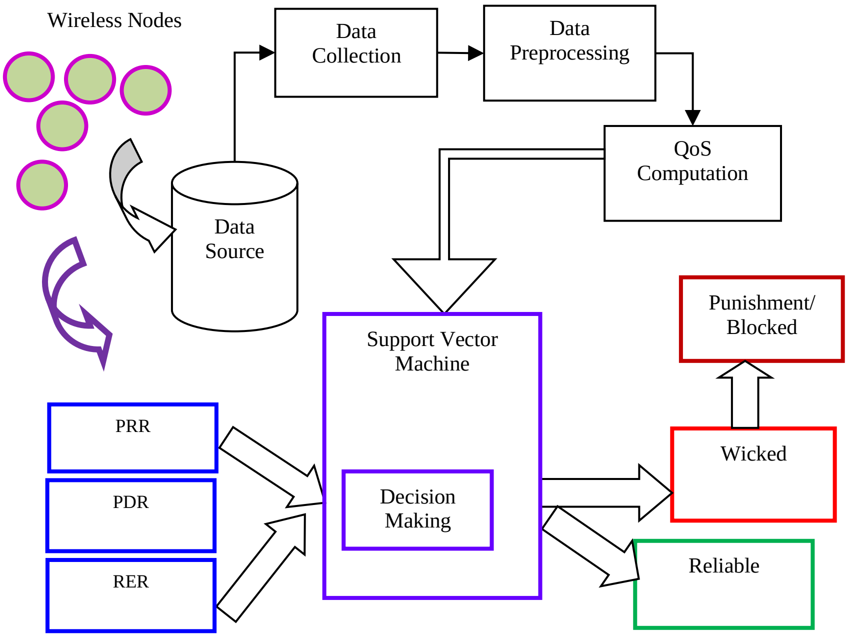

Figure 1. The architecture of the SVMD approach

Then the significant task of the QoS computation phase is to calculate the QoS of the node established on the packet received ratio (PRR), packet delay ratio (PDR), and remaining energy ratio (RER). The SVM categorization phase is dependable for categorizing the node as reliable, medium honest, and wicked. Lastly, the major dependability of the decision-making process is to keep track of the introduced system and allocate the punishment in terms of blocking the wicked nodes.

2.1. Data collection phase

In this phase, the wireless nodes observe the surrounding information at a definite period and assemble the essential data. The attributes are collected based on features of mobility and packet. The experiments are approved by applying the data source gathered from the network. Route request (RREQ) and route reply (RREP) messages are illustrated in the packet-established attribute set. In RREQ, the sender forwards the RREQ message to near neighbor nodes, and this procedure ends till the receiver receives the message. Then the receiver delivers the RREP message back to the sender. Then the sender forwards the data through this path.

2.2. Data preprocessing phase

The observing information usually reveals spatial and temporal redundancies because of the spatial and temporal connection between the observed information. Thus, in this approach, the regression model is applied to eliminate the connection in WANET. The preprocessing data phase is significant and essential since this phase, features used in the system are unnecessary attributes that are rejected. The important objective of this phase is to remove the subset of attributes that plays an input in raising the system with enhanced function and improved accuracy. The unnecessary and imperfect information is undisturbed from the dataset during the attribute's removal procedure. In addition, it minimizes energy utilization during data transmission and enhances the network lifetime. Here, the LCC method reduces the number of features. The LCC method is extremely rapid and perfect and measures the connection between two nodes. The LCC concerning x and y can be calculated using (1).

$$Corr(x,y) = \frac{\sum_{j=1}^{n}(x_{j-}x)(y_{j-}y)}{\sqrt{\sum_{j=1}^{n}(x_{j-}x)^2 \sum_{j=1}^{n}(y_{j-}y)^2}} \tag{1}$$

The connection between x and y is decided by the $corr(x,y)$ value, which lies between -1 to 1. The value near 0 represents that the relationship between x and y is weak, and near 1 represents a strong connection between x and y. This approach aims to recognize the wicked nodes and remove unnecessary features. The feature selection is specified by (2).

$$F_{corr} = Max\big(corr(class;sf)\big) - \frac{1}{|EFS|}\sum_{sf\in EFS}\frac{Corr(sf;f)}{Corr(Class;sf)} \tag{2}$$

Here, F_{corr} denotes the feature correlation, sf indicates the set of features, and EFS represents the extracted feature subset. If feature correlation (F_{corr}), $F_{corr} = 0$, the node features are unnecessary for the class (CL). Hence, the node features are rejected. If $F_{corr} < 0$ represents that the node features are disproportionate to the class CL, the feature node features are dismissed. If $F_{corr} > 0$ means the applicable node feature offers information about the output class CL. Thus, the node features are upended in the extracted feature subset (EFS).

$$E = exp\left[\frac{1}{\frac{1+(IE-(RE-TE))}{IE}}\right] \tag{3}$$

2.3. QoS computation phase

Here, the QoS value of a node is evaluated through performance analysis like PRR, PDR, and RER. These metrics decide whether the node is wicked or reliable in the network. PRR is the ratio of packets received to the whole count of forwarding packets from the sender. PDR is defined as the difference between the received packet time and the delivered packet time. RER is defined as the difference between initial energy and utilized energy. PRR PDR, RER metrics calculations are shown in (4), (5), (6), and packet received ratio threshold (PRR_{TH}), packet delivery ratio threshold (PDR_{TH}), remaining energy ratio threshold (RER_{TH}) computations are described in (7), (8), (9). Where k indicates the node count and PRR_{TH}, PDR_{TH}, and RER_{TH} denote the PRR, PDR, and RER threshold.

$$PRR = \frac{Count\ of\ received\ pacets}{Whole\ count\ of\ forwarding\ packets} \tag{4}$$

$$PRR = Received\ Packet\ Time - Forwarded\ Packet\ Time \tag{5}$$

$$RER = Initial\ Energy - Utilized\ Energy \tag{6}$$

$$PRR_{TH} = \sum_{i=1}^{K}\frac{PRR(k)}{k} \tag{7}$$

$$PDR_{TH} = \sum_{i=1}^{K}\frac{PDR(k)}{k} \tag{8}$$

$$RRR_{TH} = \sum_{i=1}^{K} \frac{RER(k)}{k} \tag{9}$$

2.4. SVM-based categorization phase

SVM is a type of supervised machine learning and the primary classification model. The SVM is an appropriate algorithm for detecting wicked nodes and reaches high recognition accuracy. Therefore, the detection module measured in this approach is residential by applying SVM-based learning. It executes linear and nonlinear classification. SVM-based categorization is used to categorize the nodes as reliable or wicked nodes. In this approach, the node QoS factor mitigates several attacks from the network. Initially, the SVM is trained with EFS and the node QoS, specifically PDR, PDR, and RER. The SVM-based node categorized is specified in (10).

$$Variation = \left(\sum_{i=1}^{K} \left|x_j - y_j\right|\right) \tag{10}$$

Here, x_j and y_j denote the nodes x and y features. It means the variation in the values between nodes of categorization. The nodes are categorized by wicked or reliable. We compare the node QoS metrics between the node x and y PRR, PDR, and RER values. If the node PRR value is lesser than the threshold value; the node PDR value is greater than the threshold value, and the RER value is greater than the threshold value that node is a wicked node. Finally, give the punishment based on performance to the wicked nodes to block the temporally or permanent function from the route in the WANET. An SVMD approach algorithm is specified below.

Algorithm. Algorithm for SVMD approach

```
start
input: wireless nodes, sender, receiver
output: wicked node detection, receiver reaches the data efficiently
wicked node detection procedure
data collection phase
gathering surrounding information
data preprocessing phase
LCC method do
minimizes the features
QoS computation phase
compute PRR
compute PDR
compute RER
node categorization phase
SVM algorithm do
wicked nodes ==> punishment or blocked
reliable nodes ==> data transmission
end
```

3. SIMULATION ANALYSIS

This paper uses the network simulator ns-2.35 to measure the network performance of the PITrust and SVMD approaches. Here, 100 wireless nodes are used to measure the network performance, and these nodes move arbitrarily. This approach uses 802.11 medium access control (MAC) for execution. The wireless nodes' transmission range is 180 m, and several wicked nodes are arbitrarily distributed in the field [29]. To evaluate the execution of the introduced approach, wireless sensor nodes speed from 1 m/s and 10 m/s correspondingly [30]. The function of the SVMD is measured by RER, PDR, PRR, and the possibility of miss detection ratio of routing. The performance of the SVMD approach is also deliberated by examining the PRR. PRR is the ratio of the total amount of data packets obtained to the amount of data packets forwarded. Figure 2 explains the execution of the PITrust and SVMD approaches for the PRR.

The SVMD approach detects the wicked nodes by the SVM algorithm. This technique makes an intelligent decision for separating reliable nodes by node PRR, PDR, and RER. Thus, the SVMD approach detects the wicked nodes efficiently. But, the PITrust approach does not detect the wicked nodes efficiently. As a result, it minimizes the network PRR in the network. From Figure 3, the SVMD approach minimizes the delay in the network. In SVMD, the LCC method reduces the number of features.

The SVMD approach utilizes a SVM algorithm to detects the wicked nodes efficiently. As a result, it minimized the network delay. Though, the PITrust approach raises the delay compared to the SVMD approach. RER is defined as the amount of energy remaining in a network. Figure 4 explains the PITrust and SVMD approaches for the RER. During data transmission, the nodes' energy is utilized when packets are forwarded to the receiver. Figure 4 illustrates that the SVMD approach has the highest remaining energy than the PITrust approach.

This approach uses the SVM algorithm to improve the network's wicked node detection. But, the PITrust approach reduces the energy preservation in the network. Miss detection is defined as the possibility that this system wrongly detects the wicked nodes. Figure 5 explains the PITrust and SVMD approaches for the miss detection possibility. The possibility of miss detection is deviated based on the count of WANET nodes.

From Figure 5, the proposed SVMD approach has a lesser miss detection possibility since the SVM algorithm is used to detect wicked nodes efficiently. The SVM mechanism separates the wicked nodes based on PRR, PDR and RER metrics. However, the PITrust approach raises the miss detection by increasing the WANET nodes since it cannot notice the wicked nodes.

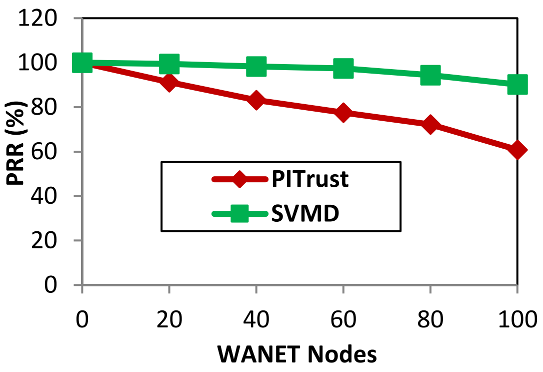

Figure 2. PITrust and SVMD approaches for PRR

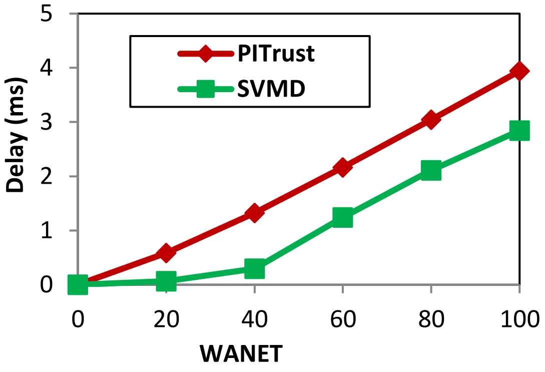

Figure 3. PITrust and SVM-DWN approaches for PDR

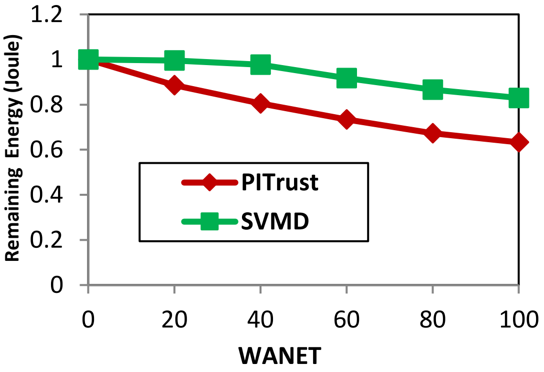

Figure 4. PITrust and SVMD approaches for RER

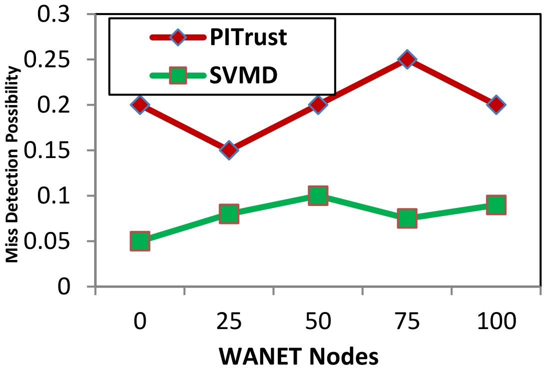

Figure 5. PITrust and SVMD approaches for miss detection possibility

4. CONCLUSION

WANET communication is vulnerable to several types of attacks. The SVM-based wicked node detection in WANET is introduced in this paper. This article uses an SVMD approach to diminish the wicked nodes in IoT WANET and improve detection accuracy. This approach contains a data collection phase, data preprocessing phase, QoS computation phase, and SVM-based categorization phase. Here, the LCC method operates to minimize unnecessary data; thus, it reduces the network delay. The SVM algorithm categorized the wicked or reliable nodes based on node performance like PRR, PDR, RER, and miss detection possibility ratio. The simulation results analyzed the version of the SVMD with PITrust approaches using a network simulator. This approach provided better efficiency and improved energy efficiency. The simulation results demonstrated that the SVMD system provided better detection performance. Furthermore, the SVMD approach minimized the network delay. However, this paper increases the little packet loss ratio due to congestion. In future, we use Resource allocation concept for reducing the packet loss ratio in the network. Furthermore, we use the artificial intelligence learning algorithm to improve the routing efficiency in future.

REFERENCES

[1] S. Selvarasu, K. Bashkaran, K. Radhika, S. Valarmathy, and S. Murugan, "IoT-enabled medication safety: Real-time temperature and storage monitoring for enhanced medication quality in hospitals," in *2023 2nd International Conference on Automation, Computing and Renewable Systems (ICACRS)*, Dec. 2024, pp. 256–261, doi: 10.1109/icacrs58579.2023.10405212.

[2] R. K. Vanakamamidi, N. Abirami, C. Sasi Kumar, L. Ramalingam, S. Priyanka, and S. Murugan, "IoT security based on machine learning," in *2023 2nd International Conference on Smart Technologies for Smart Nation, SmartTechCon 2023*, Aug. 2023, pp. 683–687, doi: 10.1109/SmartTechCon57526.2023.10391727.

[3] K. Ghanem, F. J. Aparicio-Navarro, K. G. Kyriakopoulos, S. Lambotharan, and J. A. Chambers, "Support vector machine for network intrusion and cyber-attack detection," in *2017 Sensor Signal Processing for Defence Conference, SSPD 2017*, Dec. 2017, vol. 2017-Janua, pp. 1–5, doi: 10.1109/SSPD.2017.8233268.

[4] B. Meenakshi, B. Gopi, L. Ramalingam, A. Vanathi, S. Sangeetha, and S. Murugan, "Wireless sensor networks for disaster management and emergency response using SVM classifier," in *2023 2nd International Conference on Smart Technologies for Smart Nation, SmartTechCon 2023*, Aug. 2023, pp. 647–651, doi: 10.1109/SmartTechCon57526.2023.10391435.

[5] P. Gu, R. Khatoun, Y. Begriche, and A. Serhrouchni, "Support vector machine (SVM) based sybil attack detection in vehicular networks," Mar. 2017, doi: 10.1109/WCNC.2017.7925783.

[6] M. S. Khan, L. Khan, N. Gul, M. Amir, J. Kim, and S. M. Kim, "Support vector machine-based classification of malicious users in cognitive radio networks," *Wireless Communications and Mobile Computing*, vol. 2020, pp. 1–11, Jul. 2020, doi: 10.1155/2020/8846948.

[7] J. D. Kim, M. Ko, and J. M. Chung, "Physical identification based trust path routing against sybil attacks on RPL in IoT networks," *IEEE Wireless Communications Letters*, vol. 11, no. 5, pp. 1102–1106, May 2022, doi: 10.1109/LWC.2022.3157831.

[8] X. Huang and Y. Wu, "Identify selective forwarding attacks using danger model: Promote the detection accuracy in wireless sensor networks," *IEEE Sensors Journal*, vol. 22, no. 10, pp. 9997–10008, May 2022, doi: 10.1109/JSEN.2022.3166601.

[9] V. S. R, "Support vector based regression model to detect sybil attacks in WSN," *International Journal of Advanced Trends in Computer Science and Engineering*, vol. 9, no. 3, pp. 4090–4096, Jun. 2020, doi: 10.30534/ijatcse/2020/236932020.

[10] Y. Lai *et al.*, "Identifying malicious nodes in wireless sensor networks based on correlation detection," *Computers and Security*, vol. 113, Art. no. 102540, Feb. 2022, doi: 10.1016/j.cose.2021.102540.

[11] X. Yin and S. Li, "Trust evaluation model with entropy-based weight assignment for malicious node's detection in wireless sensor networks," *Eurasip Journal on Wireless Communications and Networking*, vol. 2019, no. 1, Aug. 2019, doi: 10.1186/s13638-019-1524-z.

[12] J. Ding, H. Wang, and Y. Wu, "The detection scheme against selective forwarding of smart malicious nodes with reinforcement learning in wireless sensor networks," *IEEE Sensors Journal*, vol. 22, no. 13, pp. 13696–13706, Jul. 2022, doi: 10.1109/JSEN.2022.3176462.

[13] R. Raman, R. Jagtap, S. Muthumarilakshmi, M. Lalitha, G. Jethava, and S. Murugan, "Energy monitoring in solar-powered buildings using internet of things," in *2023 Second International Conference on Smart Technologies for Smart Nation (SmartTechCon)*, Aug. 2023, pp. 318–322, doi: 10.1109/SmartTechCon57526.2023.10391826.

[14] A. Ghani, K. Mansoor, S. Mehmood, S. A. Chaudhry, A. U. Rahman, and M. Najmus Saqib, "Security and key management in IoT-based wireless sensor networks: An authentication protocol using symmetric key," *International Journal of Communication Systems*, vol. 32, no. 16, Sep. 2019, doi: 10.1002/dac.4139.

[15] M. U. Rana, O. Elahi, M. Mushtaq, and M. A. Shah, "Identity based cryptography for Ad Hoc networks," in *IET Conference Proceedings*, 2022, vol. 2022, no. 8, pp. 93–98, doi: 10.1049/icp.2022.2047.

[16] D. Verchyk and J. Sepúlveda, "Towards post-quantum enhanced identity-based encryption," in *Proceedings - 2021 24th Euromicro Conference on Digital System Design, DSD 2021*, Sep. 2021, pp. 502–509, doi: 10.1109/DSD53832.2021.00081.

[17] R. Qazi, K. N. Qureshi, F. Bashir, N. U. Islam, S. Iqbal, and A. Arshad, "Security protocol using elliptic curve cryptography algorithm for wireless sensor networks," *Journal of Ambient Intelligence and Humanized Computing*, vol. 12, no. 1, pp. 547–566, Apr. 2021, doi: 10.1007/s12652-020-02020-z.

[18] S. Lingeshwari and R. Natchadalingam, "Provisioning of efficient authentication technique for implementing in large scale networks (PEAT)," *International Journal of MC Square Scientific Research*, vol. 6, no. 1, pp. 34–42, Jul. 2014, doi: 10.20894/ijmsr.117.006.001.006.

[19] M. Luo, Y. Luo, Y. Wan, and Z. Wang, "Secure and efficient access control scheme for wireless sensor networks in the cross-domain context of the IoT," *Security and Communication Networks*, vol. 2018, pp. 1–10, 2018, doi: 10.1155/2018/6140978.

[20] C. S. Ranganathan, R. Raman, K. K. Sutaria, R. A Varma, and S. Murugan, "Network security in cyberspace using machine learning techniques," in *2023 7th International Conference on Electronics, Communication and Aerospace Technology (ICECA)*, Nov. 2024, pp. 1755–1759, doi: 10.1109/iceca58529.2023.10394962.

[21] A. El Attaoui, S. Largo, S. Kaissari, A. Benba, A. Jilbab, and A. Bourouhou, "Machine learning-based edge-computing on a multi-level architecture of WSN and IoT for real-time fall detection," *IET Wireless Sensor Systems*, vol. 10, no. 6, pp. 320–332, Oct. 2020, doi: 10.1049/iet-wss.2020.0091.

[22] B. Trăsnea, C. Ginerică, M. Zaha, G. Măceşanu, C. Pozna, and S. Grigorescu, "Octopath: An octree-based self-supervised learning approach to local trajectory planning for mobile robots," *Sensors*, vol. 21, no. 11, Art. no. 3606, May 2021, doi: 10.3390/s21113606.

[23] R. Hussain and H. Oh, "On secure and privacy-aware sybil attack detection in vehicular communications," *Wireless Personal Communications*, vol. 77, no. 4, pp. 2649–2673, Feb. 2014, doi: 10.1007/s11277-014-1659-5.

[24] S. Madhuri and J. Mungara, "Fusion of cuckoo search and hill climbing techniques based optimal forwarder selection and detect the intrusion," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 27, no. 1, pp. 328–335, Jul. 2022, doi: 10.11591/ijeecs.v27.i1.pp328-335.

[25] W. Sun, X. Yuan, J. Wang, Q. Li, L. Chen, and D. Mu, "End-to-end data delivery reliability model for estimating and optimizing the link quality of industrial WSNs," *IEEE Transactions on Automation Science and Engineering*, vol. 15, no. 3, pp. 1127–1137, Jul. 2018, doi: 10.1109/TASE.2017.2739342.

[26] A. Unnikrishnan and V. Das, "Cooperative routing for improving the lifetime of wireless ad-hoc networks," *International Journal of Advances in Signal and Image Sciences*, vol. 8, no. 1, pp. 17–24, Jan. 2022, doi: 10.29284/IJASIS.8.1.2022.17-24.

[27] M. A. Uddin and Mamun-Or-Rashid, "Link expiration time-aware routing protocol for UWSNs," *Journal of Sensors*, vol. 2013, pp. 1–9, 2013, doi: 10.1155/2013/625274.

[28] K. N. Qureshi, S. Din, G. Jeon, and F. Piccialli, "Link quality and energy utilization based preferable next hop selection routing for wireless body area networks," *Computer Communications*, vol. 149, pp. 382–392, Jan. 2020, doi: 10.1016/j.comcom.2019.10.030.

[29] M. J. Kumar, S. Mishra, E. G. Reddy, M. Rajmohan, S. Murugan, and N. A. Vignesh, “Bayesian decision model based reliable route formation in internet of things,” *Indonesian Journal of Electrical Engineering and Computer Science (IJEECS)*, vol. 34, no. 3, pp. 1665–1673, Jun. 2024, doi: 10.11591/ijeecs.v34.i3.pp1665-1673.

[30] M. Amru *et al.*, “Network intrusion detection system by applying ensemble model for smart home,” *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 14, no. 3, pp. 3485–3494, Jun. 2024, doi: 10.11591/ijece.v14i3.pp3485-3494.

BIOGRAPHIES OF AUTHORS

Chitra Sabapathy Ranganathan is (Client partner | account management | IT transformation strategy | digital engineering solutions & advisory | Agile delivery adoption | sales | CoE & CoP Setup). Results-oriented, accomplished business technology leader with 23+ years of experience in software engineering and design. Proven track record of conceptualizing, architecting, and delivering reliable and scalable systems in a variety of areas comprising multi-technologies including. Cloud, big data, AI, ML, advance analytics, blockchain, mainframe, and business intelligence. Executed complex engagements across multiple verticals, manage sales, IT delivery and operations, established vision, strategy, and journey maps that align with business priorities. Enterprise leader in digital engineering solutions & advisory, Agile delivery adoption & management, pre-sales, CoE & CoP Setup, IT transformation strategy, enterprise quality and digital assurance. He can be contacted at email: Chitrasabapathyranganathan@gmail.com.

Rajeshkumar Sampathrajan is a principal cloud architect at McKinsey, where he leads a team of engineers and architects in designing and building highly scalable, resilient, and distributed systems using the latest cloud native technology in Google Cloud Platform (GCP). He has over 17 years of experience in the IT industry, spanning various domains such as banking, retail, healthcare, and consulting. With multiple GCP certifications, as well as credentials in Azure, Snowflake, HashiCorp, Teradata, Cloudera, and ITIL, Rajesh is an expert in cloud computing, big data, machine learning, and security. He has successfully delivered solutions for complex and large-scale data analytics, data engineering, and data science projects, leveraging GCP BigQuery, Vertex AI, Dataiku, and other tools. He is passionate about helping clients transform their businesses with data-driven insights and innovative solutions. He can be contacted at rajesampathrajan@gmail.com.